(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 août 2005 (25.08.2005)

PCT

(10) Numéro de publication internationale
WO 2005/079090 A1

(51) Classification internationale des brevets[7] : H04Q 7/32, 7/38

(21) Numéro de la demande internationale :
PCT/FR2005/000328

(22) Date de dépôt international :
11 février 2005 (11.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0401347 11 février 2004 (11.02.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

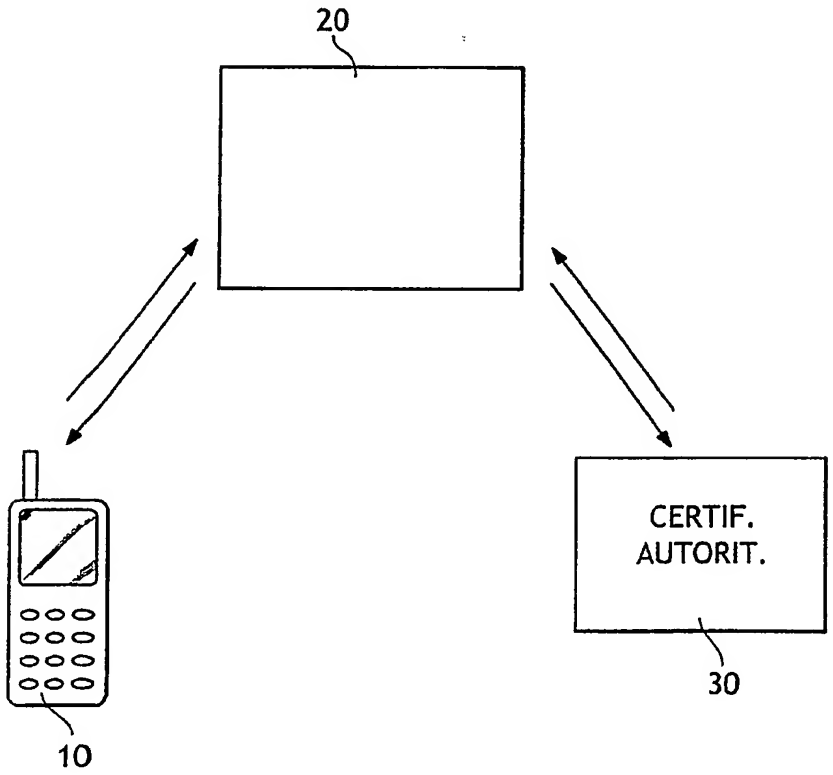
(75) Inventeurs/Déposants *(pour US seulement)* : **ARDITTI, David** [FR/FR]; 46ter, rue Paul Vaillant Couturier, F-92140 Clamart (FR). **LABBE, Bruno** [FR/FR]; 13, rue Gustave Courbet, F-78370 Plaisir (FR). **BEGAY, Didier** [FR/FR]; Villeneuve, F-16430 Champniers (FR).

(74) Mandataires : **JOLY, Jean-Jacques** etc.; Cabinet Beau de Loménie, 158, rue de l'Université, F-75340 Paris Cedex 07 (FR).

[Suite sur la page suivante]

(54) Title: EMISSION OF A PUBLIC KEY BY A MOBILE TERMINAL

(54) Titre : EMISSION DE CLE PUBLIQUE PAR UN TERMINAL MOBILE



30 ... CERTIF. AUTHORITY

(57) **Abstract:** The invention relates to a method of certification involving a public key certification authority (30) and at least one mobile terminal (10) which can receive messages which are encrypted by said public key, characterized in that it comprises a stage which consists in generating the public key in the mobile terminal (10), a stage wherein a telecommunications network entity (20) acquires said key from the terminal (10) by means of a network communication, and a stage wherein the terminal (10) is authenticated for the network entity by means of an authentication process of the interlocutor used in a conventional telephone communication, said method comprising a stage wherein the public key is supplied to the certification authority (30) along with the result of the identification process.

[Suite sur la page suivante]

WO 2005/079090 A1

(81) **États désignés** *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** L'invention concerne un procédé de certification faisant appel à une autorité de certification (30) de clé publique et faisant appel à au moins un terminal mobile (10) apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape consistant à générer la clé publique au sein du terminal mobile (10) lui-même, l'étape consistant, pour une entité (20) de réseau de télécommunications à acquérir cette clé auprès du terminal (10) par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal (10) par un processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification (30) cette clé publique en association avec le résultat de ce processus d'identification.